302 – SKYPE COMMUNICATIONS LOGS

TEAM INFORMATION

Team Name: Barely Legal

Results Email: [redacted]

Examination Time Frame: to 10/31/08

INSTRUCTIONS

Description: Examiners must develop and document a methodology used to parse SKYPE communication logs from the communication/program files in the **302_SKYPE_Communications_Logs_Challenge2008** folder to an easily understandable, viewable, and readable rendering of the communications (remove non-conversation data). The supplied files were from either or both of the two computers used in the chat conversation. A detailed explanation of your process (software or technique) used to examine, extract, and present the data is required.

Points will be awarded for the completeness of the data recovered from the communications and the ease of understanding or utility of the method the information is reported from that file(s).

Total Weighted Points: 60 Total Points available per entry – Total 300 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

INTERNAL REVIEWER USE ONLY

Reviewer:	Points Awarded:
Date:	Review Period: to

Completed: ☐ Yes ☐ No ☐ Partial

302 – SKYPE Communications Logs

Two conversation logs were recovered and extracted from the "302_SKYPE_Communications_Logs_Challenge2008" folder. They are entitled "chatmsg256" and chatmsg512". The reformatted contents are shown below:

(chatmsg256.dbb)

Communication between: kiki1932 and yogibear1953

```
From: kiki1932
yogibear1953
Bob Zeus


From: kiki1932
hey, it's me, you there?
Bob Zeus


From: yogibear1953
yea, i'm here, what's up?
Blane Stallman


From: yogibear1953
hold on, got an important phone call.  i'll get back with u
Blane Stallman


From: kiki1932
Bob Zeus
yogibear1953

From: kiki1932
yogibear1953
Bob Zeus


From: kiki1932
Bob Zeus
kiki1932 yogibear1953



From: yogibear1953
So Bob, what's happening, you haven't been on in awhile?
Blane Stallman


From: kiki1932
Sorry, been taking care of all the other business herer, didn't have the time.
Bob Zeus
```

From: yogibear1953
sorry didn't think about the name thing just nervous I guess
Blane Stallman

From: kiki1932
Jut think about what your going to do with all that money and youll feel better soon
Bob Zeus

From: yogibear1953
Blane Stallman
yogibear1953

From: kiki1932
you got the weapons and other gear?
Bob Zeus

From: kiki1932
Will he get wise?
Bob Zeus

From: kiki1932
Didn't leave any traces you were ther and took them out
Bob Zeus

From: kiki1932
How bout the ammo?
Bob Zeus

From: yogibear1953
I just went down and bought some new
Blane Stallman

From: kiki1932
Didn't have to give them a name or anything did you?
Bob Zeus

From: yogibear1953
Nope, just like buying steaks at the grocery
Blane Stallman

From: kiki1932
Good, how bout the rest of the swtufff
Bob Zeus

From: kiki1932
Didn't buy new
Bob Zeus

From: yogibear1953
When we hit this place its going to be empty right?
Blane Stallman

From: kiki1932
Settle down. If we stick to the plan and do this right theyrll be no problems
Bob Zeus

From: yogibear1953
Yea, that's what you say now, but that's not the way it worked out last time
Blane Stallman

From: yogibear1953
Don't change a thing man, you still killed them
Blane Stallman

From: kiki1932
Sorry, jut the pressure, I know you won't and didn't talk
Bob Zeus

From: yogibear1953
Ok man, later
Blane Stallman

From: kiki1932
later
Bob Zeus

(chatmsg512.dbb)

Communication between: kiki1932 and yogibear1953

From: yogibear1953
You know we still have that time thing going on, we miss our chance and we're out of luck this time, maybe for a long time
Blane Stallman

From: kiki1932
you know, we shouldn't be using names int htis converstion and yea I know about the time thing but we gotta be careful man
Bob Zeus

From: yogibear1953
Yea, thought I was going to have a problem with the guns, by my uncle's a hunter and had a lot so I just "borrowed" some from him
Blane Stallman

From: yogibear1953
Naw, he keps them in the basement and hasn't used them in years. they were in an old metal cabinet, dusty and dirty as all get out
Blane Stallman

From: yogibear1953
Nope, used a rag over my nands and blew some dust back over where they had been sitting. Things were a pain to clean though
Blane Stallman

From: yogibear1953
Got an old can of black powder from his basement also, maybe 30 pounds, old but never been opened, should still be good
Blane Stallman

From: yogibear1953
They would have wanted ID for that man, and I only have the one fake set and I didn't want to burn it on that
Blane Stallman

From: kiki1932
Good, whit what I got out of the anarchists cookbook combined with that were going to open some eyesw I'll tell you that
Bob Zeus

From: kiki1932
Except for some roving security and I told you I scoped that out and timed them up. Always taking lunc together at the same time so we got an hour
Bob Zeus

From: yogibear1953
I just don't want any mistakes. It's one thing to do this but murder, man they sick a needle in your arm and that stuff burning is the last thing you feel
Blane Stallman

From: kiki1932
That was justt bad luck, and it was bad luck for them. I didn't want anyone to get hurt, you know that
Bob Zeus

From: kiki1932
Listen amigo you were right there too and unless you shut up and follwo the plan well both be looking a a ride on the needle SO SHUT YOUR MOUTH ABOUT THE LAST JOB
Bob Zeus

From: yogibear1953
Don't talk to me that way. I've been loyal and haven't said a thing. I know they're still looking for who pulled that and that means us. I aint gonna help them kill me
Blane Stallman

From: kiki1932
listen, we got this going and just need to chill awhile. Gotta get off this comm and get on the other one we set up so they cant trace us so good. Get up on that one, regular time and well finish the planning
Bob Zeus

METHODOLOGY / NOTES FORM

302 – SKYPE Communications Logs

Date / Time	Notes
26-Oct-08 4:00 pm	Tool(s) Used: Linux OS commands: `strings, md5sum` Custom Perl script (attached with this report as file "302-clean.pl") Located Skype Communication Log files in each of the three directories. Confirmed that the Skype chat logs were identical in the "2 yogibear1953" and "Skype2" folders by verifying the MD5 hash values using `md5sum` Ran `strings` command on relevant .dbb files. Created perl script (302-clean.pl) to extract and reformat relevant data.

```
#!/usr/bin/perl

#$thefile="chatmsg256.dbb.str";
$thefile="chatmsg512.dbb.str";

open (FILE,"<$thefile");
@all_lines = <FILE>;
close FILE;

$thefile .= ".txt";
open (FILE,">$thefile");
$i=13;
foreach $line (@all_lines) {
if ($line  =~ /^#/)
{
        $line =~ s/#/Communication between: /;
        $line =~ s/\/\$/ and /;
        $line =~ s/\;.*$/\n\n/;
        print FILE $line if ($g < 1);
        $i=0;
        $g=1;
}
#elsif ($line =~ /^\d*/) {}

print FILE "From: " . $line if ($i==1);
print FILE $line if ($i==2);
print FILE $line if ($i==3);
if ($i > 3)
{
print FILE "\n";
}

$i++;


}
close FILE;
```